C8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,015	09/27/2001	Vincent J. Zimmer	42390P11198	4663

7590 06/29/2005

Tom Van Zandt
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
PROCTOR, JASON SCOTT	

ART UNIT	PAPER NUMBER
2123	

DATE MAILED: 06/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/966,015	**Applicant(s)** ZIMMER, VINCENT J.	
	Examiner Jason Proctor	**Art Unit** 2123	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 March 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,7-9,11,15,17 and 21-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,7-9,11,15,17,21-27,30-35 and 37* is/are rejected.

7)☒ Claim(s) *28,29 and 36* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 March 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 1-20 were presented for examination and rejected in Office Action dated December 21, 2004. Applicant has amended claims 1-3, 7-9, 11, 15, and 17; cancelled claims 4-6, 10, 12-14, 16, and 18-20; and added new claims 21-37 in response dated March 21, 2005. Claims 1-3, 7-9, 11, 15, 17, and 21-27 are currently pending.

Claims 1-3, 7-9, 11, 15, 17, 21-27, 30-35, and 37 have been rejected.

Summary of the Rejections and Objections

Claims 1-3, 7-8, 9, 11, 15, 17, 21-26, 33-34, and 37 stand rejected under 35 U.S.C. §§ 102 or 103 as being anticipated or unpatentable over the prior art made of record.

Claims 7, 8, 24, 25, 30-33, and 35 stand rejected under 35 U.S.C. § 112 for indefinite limitations related to the use of the term "enables".

Claim 25 stands rejected under 35 U.S.C. § 112 for indefinite limitations related to a method that fails to positively recite acts to be performed.

Claims 27, 30, 32, and 35 stand rejected under 35 U.S.C. §§ 101 and/or 112 for reciting indefinite use limitations.

Claims 28-29 and 36 are objected to.

Response to Objections to the Drawings

The Examiner thanks Applicant for entering substitute drawing sheets in response to the objections to the drawings of the previous Office Action. The Examiner concurs that no new matter has been entered. The previous objections to the drawings have been withdrawn.

Response to Rejections under 35 U.S.C. § 112

Regarding the previous rejections of claims 5, 6, 13, 14, 19, and 20 under 35 U.S.C. § 112, first paragraph, Applicant has cancelled these claims. Therefore the previous rejections under 35 U.S.C. § 112, first paragraph, are moot and have been withdrawn.

Regarding the previous rejections of claims 7 and 8 under 35 U.S.C. § 112, second paragraph, although Applicant has not presented arguments regarding these claims, the amendments to the claims obviate the previous rejections. Therefore the previous rejections under 35 U.S.C. § 112, second paragraph, have been withdrawn.

Response to Rejections under 35 U.S.C. § 101

Regarding the previous rejections of claims 1-20 under 35 U.S.C. § 101, although Applicant has not presented arguments regarding these claims, the amendments to the claims obviate the previous rejections. Therefore the previous rejections under 35 U.S.C. § 101 have been withdrawn.

Response to Rejections under 35 U.S.C. §§ 102 and 103

Regarding the previous rejections of claims 1-20 under 35 U.S.C. §§ 102 and 103, Applicant argues that the references relied upon neither anticipate nor render obvious the claimed invention. In light of the amendments, cancellations, and newly added claims, the Examiner finds this argument persuasive. The previous rejections under 35 U.S.C. §§ 102 and 103 have been withdrawn.

Outstanding Rejections and Objections

Claim Objections

1. Claims 11 and 17 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to refer to back to another pending claim. Claim 11 depends from cancelled claim 10. Claim 17 depends from cancelled claim 16. In telephone interview conducted on June 14, 2005, Mr. R Alan Burnett, Registration No. 46,149 indicated that these claims should depend from 9 and 15 respectively. The Examiner has interpreted the limitations of these claims accordingly.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 7-8, 24, 25, 30-33, and 35 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 7 recites a virtual machine monitor "that enables firmware to be provided from third parties," which renders the claim indefinite. The claim does not positively recite any interaction with firmware provided from third parties. It is unclear whether "firmware to be provided from third parties" is the same as "untrusted firmware code". It is unclear whether the metes and bounds of this claim include actually executing firmware to be provided from third parties.

Claims 8, 24, and 25 stand rejected by virtue of their dependence.

Claims 30, 33, and 35 suffer problems similar to claim 7 regarding the phrase "that enables third-party firmware modules to be loaded".

Claims 31 and 32 stand rejected by virtue of their dependence.

3. Claim 25 is further rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 25 recites two steps of "determining", neither of which positively recite any subsequent steps to be performed on the basis of the determinations. As a result, there is no indication whether these steps have any functional significance in the claimed method. It is unclear how to assign any patentable weight to the recited steps or how to identify a functionally equivalent step in the prior art.

4. Claim 27 provides the use of a VMM for authenticating an EFI firmware module, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced. There is no intrinsic or inherent capability of a VMM that provides for "authenticating an EFI firmware module". Note that claim 28 recites steps to achieve "authenticating".

Claim 27 is rejected under 35 U.S.C. § 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. § 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd.App. 1967) and *Clinical Products, Ltd.* v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. § 101 (nonstatutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

5. Claim 30 provides for the use of a VMM for authenticating a firmware module, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

There is no intrinsic or inherent capability of a VMM that provides for "authenticating an EFI firmware module". Claim 32 is rejected for the same reasons as claim 30. Claim 31, however, recites steps to achieve "authenticating". Although these claims depend from claim 9, reciting a machine-readable medium, they relate to the operations performed by the processor, and thus attempt to define a method performed by the processor.

6. Claim 35 provides for the use of a firmware component employed to authenticate firmware modules, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced. There is no intrinsic or inherent capability of a firmware module that provides for "authenticating firmware modules". Although claim 35 depends from claim 15, reciting an apparatus, it relates to the operations performed by the apparatus, and thus attempts to define a method performed by the apparatus.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-3, 9, 11, 15, 17, 22, and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent No. 6,397,242 to Devine et al. (Devine), reference made of record on form PTO-892 mailed with the previous Office Action.

Regarding claim 1, Devine teaches VMMs and the use of a VMM to emulate legacy hardware components, both of which are recited by the claim:

- Implementing a virtual machine monitor (VMM) upon a computer system having a native environment that executes in physical mode [*"One solution that was the subject of intense research in the late 1960's and 1970's came to be known as the 'virtual machine monitor' (VMM)"* (column 1, lines 36-52); *"Virtual machine monitors can also provide architectural compatibility between different processor architectures by using a technique known as either 'binary emulation' or 'binary translation'."* (column 2, lines 21-35)]; and
- Emulating legacy hardware components that are not present in the native environment using the VMM to provide support for legacy code that presupposes the existence of such hardware components [*"Virtual machine monitors (VMM) have many attractive properties.* [...] *Furthermore, they allow modern operating systems to coexist, not just the legacy operating system that legacy virtual machine monitors allow.* (column 4, lines 23-36)].

Devine also teaches an invention comprising a VMM [*"The invention comprises a hardware processor; a memory; a virtual machine monitor (VMM); and a virtual machine*

(VM)." (column 5, lines 11-19)]. Devine's invention operates upon a computing system having a native environment that executes in physical mode [*"The virtual machine 120 then will also include the virtual operating system (VOS) 700, which communicates with the "real," or "physical" system hardware 710 via the VMM 100."* (column 24, lines 39-51)].

Devine does not expressly teach that the VMM is "firmware-based", however Devine does teach that the VMM does not require a host operating system [*"Fig. 8 is a block diagram that illustrates the fact that invention – switching between binary translation and direct execution modes – does not require a host operating system."* (column 24, lines 60-67)]. The significance of a VMM that does not require a host operating system is explained by Applicants' arguments (page 12):

> Clearly, this conventional legacy VMM [taught by Bugnion] is not firmware-based, but rather runs on top of an existing operating system or is part of an existing operating system. This is significant because a software application used to access hardware runs significantly slower than firmware components used to access the same hardware since **the software application is layered on an operating system, which, in turn, is layered over a firmware layer sitting between the operating system and the hardware.** (emphasis added)

Devine expressly teaches a VMM corresponding to Applicants' arguments, that is, a VMM that does not require an operating system, which implicitly discloses a VMM that is not a software application, is not layered on an operating system, and which therefore resides at the firmware level directly on the hardware.

Claim 9 recites a machine-readable medium that provides executable instructions for performing the method of claim 1. As Devine's invention is computer implemented (column 5, lines 11-19) and corresponds to Applicants' arguments regarding a firmware implementation (see rejection of claim 1 above), claim 9 stands rejected for the same reasons given for claim 1.

Claim 15 recites an apparatus comprising a computer system that performs a broader recitation of the method of claim 1. As Devine's invention is computer implemented, thus an apparatus, (column 5, lines 11-19) claim 9 stands rejected for the same reasons given for claim 1.

Regarding claims 2 and 3, Devine teaches that the native environment is a 32-bit environment [*"The invention is particularly well-suited for virtualizing computer systems in which the hardware processor has an Intel x86 architecture that is compatible with at least the Intel 80386 processor."* (column 6, lines 53-56)] and provides at least PC/AT environment emulation [*"Moreover, the Intel x86 architecture contains, in addition to its protected, fundamental or 'native' mode, a non-native mode of operation such as 'real mode,' 'virtual 8086 (v-8086) mode,' and 'system management mode.'* [...] *The invention includes a virtualization mechanism for the processor even in this case."* (column 10, lines 4-13)].

Claim 11 recites a machine-readable medium corresponding to the method of claim 3. As Devine's invention is computer implemented, as indicated in the rejection of claim 9, claim 11 stands rejected for the same reasons given for claim 3.

Claim 17 recites an apparatus corresponding to the method of claim 3. As Devine's invention is computer implemented, as indicated in the rejection of claim 15, claim 11 stands rejected for the same reasons given for claim 3.

Regarding claim 22, Devine teaches that the VMM publishes an environment that appears to be a physical mode environment [*"Moreover, the Intel x86 architecture contains, in addition to its protected, fundamental or 'native' mode, a non-native mode of operation such as 'real mode,' 'virtual 8086 (v-8086) mode,' and 'system management mode.'* [...] *The invention includes a virtualization mechanism for the processor even in this case."* (column 10, lines 4-13)]. The recited limitations of "wherein the physical mode environment includes a memory map that includes memory addresses below one megabyte, while the VMM is implemented on a computer system that does not decode physical addresses below one megabyte" are regarded as inherent details of what is known in the art as "physical mode".

Regarding claim 26, Devine teaches that the VMM performs the further operation of hiding a portion of an address space for the computer system [*"However, the VMM sets up the processor with reduced privileges so that the effect of these instructions is guaranteed to be contained to the virtual machine. For example, the VMM can never allow the processor to be effectively set at the lowest (most) privileged level, even when the operating system in the virtual machine requests it."* (column 10, lines 51-59)]. The concepts of memory protection, segmentation faults, and virtual memory are common knowledge to a person of ordinary skill in the art of computer architecture or systems programming. Thus the teachings of Devine anticipate the recited limitation of claim 26.

Please see *In re Graves*, 36 USPQ2d 1697 (CA FC 1995), quoting *In re LeGrice*, 301 F.2d 929, 133 USPQ 365 (CCPA 1962) (A reference anticipates a claim if it discloses the claimed invention "such that a skilled artisan could take its teachings in *combination with his own knowledge of the particular art and be in possession of the invention.*" *Id.* at 936, 133 USPQ at 372 (emphasis in original)); *In re Donohue*, 766 F.2d 531, 533, 226 USPQ 619, 621 (Fed. Cir. 1985) (same) (citing *In re LeGrice*, 301 F.2d at 939, 133 USPQ at 373-374).

Claim Rejections - 35 USC § 103

8. Claims 21 and 23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine as applied to claims 1 and 2, respectively, in view of "Extensible Firmware Interface Specification Version 1.02" by Intel Corporation (Intel).

As an initial matter, the Examiner observes that the publication date of the Intel reference is December 12, 2000, which qualifies it as a reference under 35 U.S.C. § 102(a), and therefore not subject to the exclusions of prior art under 35 U.S.C. § 103(c).

Regarding claim 21, Devine teaches that the VMM of the invention does not require a host operating system, as noted above (column 24, lines 60-67). A person of ordinary skill in the art could take the teachings of Devine, specifically that the VMM does not require a host operating system, in combination with his own knowledge of the particular art and be in possession of the recited limitation of loading the VMM during a pre-boot phase of the computer system. Therefore, Devine anticipates loading the VMM during a pre-boot phase of the computer system. See *In re Graves*, 36 USPQ2d 1697 (CA FC 1995).

However, Devine does not expressly teach using the invention in a computer system having an extensible firmware framework, wherein the VMM comprises a modular firmware component running on the extensible firmware framework.

Intel expressly teaches an extensible firmware framework [*"Extensible Firmware Interface Specification", "EFI",* (page 1)] that provides boot and runtime service calls that are available to the OS and its loader. Intel teaches several advantages of the EFI [*Using this formal definition, a shrink-wrap OS intended to run on Intel® architecture-based platforms will be able to boot on a variety of system designs without further platform or OS customization. The definition will also allow for platform innovation to introduce new features and functionality that enhance platform capability without requiring new code to be written in the OS boot sequence."* (page 1)]. Intel expressly teaches advantages related to Applicants' claim 1, that is, support for legacy software or devices on architecture that may not natively support the legacy software or devices [*"Furthermore, an abstract specification opens a route to replace legacy devices and firmware code over time. New device types and associated code can provide equivalent functionally through the same defined abstract interface, again without impact on the OS boot support code."* (page 1)].

It would have been obvious to a person of ordinary skill in the art at the time of Applicants' invention to combine the invention of Devine, a VMM that virtualizes an architecture to enable execution of non-native operating systems, with the teachings of Intel regarding an extensible firmware framework. Motivation to do so would be found in the teachings of Intel, particularly to improve support for a non-native "shrink-wrap OS" on the computing system using the VMM taught by Devine. Both Devine and Intel are directed, at least in part, toward support for a non-native operating system on a particular architecture. The limitations of "the VMM comprising a modular firmware component running on the extensible firmware framework" are regarded as obvious details of implementation when forming this combination; clearly the VMM of Devine would be modified to operate with the extensible firmware interface.

Regarding claim 23, Devine does not expressly teach enabling a legacy option ROM or translating the results of the I/O services into a native API.

Intel expressly teaches enabling a legacy option ROM to run and effect its input/output services ["*The PC industry has a huge investment in Intel Architecture Option ROM technology, and the obsolescence of this installed base of technology is not practical in the first generation of EFI-compliant system. The interfaces have been designed in such as way* [sic] *as to map back into legacy interfaces. These interfaces have in no way been burdened with any restrictions inherent to legacy Option ROMs.*" (page 14)].

Regarding the limitation of "translating the results of the I/O services into a native API," the disclosure of the instant application teaches (paragraph 0014):

> The VMM then translates the results [of the legacy option ROM running and effecting its I/O services] into a native API. That is, the VMM traps the I/O to the semantic equivalent in the native environment.

In a VMM which supports emulation of a non-native architecture, this is regarded as an inherent feature. Failure to perform this function would render the legacy option ROM inoperable in combination with the VMM. Therefore this limitation is an obvious detail of implementation of when combining support for a legacy option ROM with the invention of Devine.

It would have been obvious to combine support for a legacy option ROM with the invention of Devine for the reasons cited by Intel, specifically to enable support for legacy drivers which use legacy option ROMs when providing support for non-native operating system on a particular architecture. The combination would require adequate support in the VMM for the legacy devices which employ the legacy option ROMs, specifically "trapping the I/O to the semantic equivalent in the native environment". Failure to do so would produce an inoperable combination.

9. Claims 7, 8, 24, and 25 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine in view of Intel.

Regarding claim 7, Devine teaches an invention comprising a VMM [*"The invention comprises a hardware processor; a memory; a virtual machine monitor (VMM); and a virtual machine (VM)."* (column 5, lines 11-19)]. Devine teaches that the VMM of the invention does not require a host operating system, as noted above (column 24, lines 60-67). A person of ordinary skill in the art could take the teachings of Devine, specifically that the VMM does not require a host operating system, in combination with his own knowledge of the particular art and be in possession of the recited limitation of loading the VMM during a pre-boot phase of the computer system. Therefore, Devine anticipates loading the VMM during a pre-boot phase of the computer system. See *In re Graves*, 36 USPQ2d 1697 (CA FC 1995).

Devine teaches that the VMM grants access to a subset of system resources, while code access to other system resources is filtered by the VMM. [*"However, the VMM sets up the processor with reduced privileges so that the effect of these instructions is guaranteed to be contained to the virtual machine. For example, the VMM can never allow the processor to be effectively set at the lowest (most) privileged level, even when the operating system in the virtual machine requests it."* (column 10, lines 51-59)].

However, Devine does not expressly teach using the invention in a computer system having an extensible firmware framework, wherein the VMM comprises a modular firmware component running on the extensible firmware framework.

Intel expressly teaches an extensible firmware framework [*"Extensible Firmware Interface Specification", "EFI",* (page 1)] that provides boot and runtime service calls that are available to the OS and its loader. Intel teaches several advantages of the EFI [*Using this formal definition, a shrink-wrap OS intended to run on Intel® architecture-based platforms will be able to boot on a variety of system designs without further platform or OS customization. The definition will also allow for platform innovation to introduce new features and functionality that enhance platform capability without requiring new code to be written in the OS boot sequence."* (page 1)]. Intel expressly teaches advantages related to Applicants' claim 1, that is, support for legacy software or devices on architecture that may not natively support the legacy software or devices [*"Furthermore, an abstract specification opens a route to replace legacy devices and firmware code over time. New device types and associated code can provide equivalent* *functionally through the same defined abstract interface, again without impact on the OS boot support code."* (page 1)].

It would have been obvious to a person of ordinary skill in the art at the time of Applicants' invention to combine the invention of Devine, a VMM that virtualizes an architecture to enable execution of non-native operating systems, with the teachings of Intel regarding an extensible firmware framework. Motivation to do so would be found in the teachings of Intel, particularly to improve support for a non-native "shrink-wrap OS" on the computing system using the VMM taught by Devine. Both Devine and Intel are directed, at least in part, toward support for a non-native operating system on a particular architecture. The limitations of "the VMM comprising a modular firmware component running on the extensible firmware framework" are regarded as obvious details of implementation when forming this combination; clearly the VMM of Devine would be modified to operate with the extensible firmware interface.

Regarding claim 8, Devine does not expressly recite that non-native code is legacy BIOS code.

Intel expressly teaches executing legacy BIOS code [*"The EFI specification has been carefully designed to allow for existing systems to be extended to support it with a minimum of development effort. In particular, the abstract structures and services defined in the EFI specification can be supported on all legacy platforms. For example, to accomplish such support on an existing IA-32 platform that uses traditional BIOS to support operating system boot, an additional layer of firmware code would need to be provided. This extra code would be* *required to translate the existing interfaces for services and devices into support for the abstractions defined in this specification."* (page 11)].

It would have been obvious to combine support for a legacy BIOS execution with the invention of Devine for the reasons cited by Intel, specifically to enable support legacy platforms when providing support for non-native operating system on a particular architecture. The combination would require adequate support in the VMM for the legacy BIOS execution.

Regarding claim 24, Devine teaches that the VMM performs the steps of trapping attempted access to a resource, determining if the access is allowed, and subsequently allowing or denying the access [*"However, the VMM sets up the processor with reduced privileges so that the effect of these instructions is guaranteed to be contained to the virtual machine. For example, the VMM can never allow the processor to be effectively set at the lowest (most) privileged level, even when the operating system in the virtual machine requests it."* (column 10, lines 51-59); and *"A permission downgrade involves setting pages with a read-write trace to be inaccessible so that both read and write accesses lead to exceptions that are interpreted as traces. The permission downgrade sets pages with a write-only trace to be read-only, so that only writes to the page lead to faults."* (column 12, lines 34-41)].

Regarding claim 25, these limitations are rejected by virtue of the combination formed in the rejection of claim 7 in light of the rejection of claim 24. Specifically, in a VMM that operates without a host operating system on a computer system that uses extensible firmware architecture, wherein the VMM sets up the processor with reduced privileges, it would be obvious to a person of ordinary skill in the art that the same restrictions should apply regardless of whether "the firmware program is started by EFI core code". As indicated above in the rejection of claim 25 under 35 U.S.C. § 112, second paragraph, it is unclear how to assign any patentable weight to the limitations of claim 25, therefore the combination and motivation to combine in this rejection are the same as those for claim 24.

10. Claims 33 and 34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine as applied to claim 9 in view of Intel.

Regarding claim 33, Devine teaches that the VMM of the invention does not require a host operating system, as noted above (column 24, lines 60-67). A person of ordinary skill in the art could take the teachings of Devine, specifically that the VMM does not require a host operating system, in combination with his own knowledge of the particular art and be in possession of the recited limitation of loading the VMM during a pre-boot phase of the computer system. Therefore, Devine anticipates loading the VMM during a pre-boot phase of the computer system. See *In re Graves*, 36 USPQ2d 1697 (CA FC 1995).

Devine also teaches executing untrusted code on the VMM in a sandbox mode such that the code is prevented from harming the computer system [*"No code sequence executed in the virtual machine may corrupt the entire system..."* (column 9, lines 36-40); and *"The VMM then operates within the protected operation mode and uses binary translation to execute VM* *instructions whenever the real and system management operation modes of the processor are to be virtualized."* (column 7, lines 9-13)].

However, Devine does not expressly teach using the invention in a computer system having an extensible firmware framework, wherein the VMM comprises a modular firmware component running on the extensible firmware framework.

Intel expressly teaches an extensible firmware framework [*"Extensible Firmware Interface Specification", "EFI",* (page 1)] that provides boot and runtime service calls that are available to the OS and its loader. Intel teaches several advantages of the EFI [*Using this formal definition, a shrink-wrap OS intended to run on Intel® architecture-based platforms will be able to boot on a variety of system designs without further platform or OS customization. The definition will also allow for platform innovation to introduce new features and functionality that enhance platform capability without requiring new code to be written in the OS boot sequence."* (page 1)]. Intel expressly teaches advantages related to Applicants' claim 1, that is, support for legacy software or devices on architecture that may not natively support the legacy software or devices [*"Furthermore, an abstract specification opens a route to replace legacy devices and firmware code over time. New device types and associated code can provide equivalent functionally through the same defined abstract interface, again without impact on the OS boot support code."* (page 1)].

It would have been obvious to a person of ordinary skill in the art at the time of Applicants' invention to combine the invention of Devine, a VMM that virtualizes an architecture to enable execution of non-native operating systems, with the teachings of Intel regarding an extensible firmware framework. Motivation to do so would be found in the teachings of Intel, particularly to improve support for a non-native "shrink-wrap OS" on the computing system using the VMM taught by Devine. Both Devine and Intel are directed, at least in part, toward support for a non-native operating system on a particular architecture. The limitations of "the VMM comprising a modular firmware component running on the extensible firmware framework" are regarded as obvious details of implementation when forming this combination; clearly the VMM of Devine would be modified to operate with the extensible firmware interface.

Regarding claim 34, Devine does not expressly teach enabling a legacy option ROM or translating the results of the I/O services into a native API.

Intel expressly teaches enabling a legacy option ROM to run and effect its input/output services ["*The PC industry has a huge investment in Intel Architecture Option ROM technology, and the obsolescence of this installed base of technology is not practical in the first generation of EFI-compliant system. The interfaces have been designed in such as way* [sic] *as to map back into legacy interfaces. These interfaces have in no way been burdened with any restrictions inherent to legacy Option ROMs."* (page 14)].

Regarding the limitation of "translating the results of the I/O services into a native API," the disclosure of the instant application teaches (paragraph 0014):

> The VMM then translates the results [of the legacy option ROM running and effecting its I/O services] into a native API. That is, the VMM traps the I/O to the semantic equivalent in the native environment.

In a VMM which supports emulation of a non-native architecture, this is regarded as a feature required for correct operation. Failure to perform this function would render the legacy option ROM inoperable in combination with the VMM. Therefore this limitation is an obvious detail of implementation of when combining support for a legacy option ROM with the invention of Devine.

It would have been obvious to combine support for a legacy option ROM with the invention of Devine for the reasons cited by Intel, specifically to enable support for legacy drivers which use legacy option ROMs when providing support for non-native operating system on a particular architecture. The combination would require adequate support in the VMM for the legacy devices which employ the legacy option ROMs, specifically "trapping the I/O to the semantic equivalent in the native environment". Failure to do so would produce an inoperable combination.

11. Claim 37 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine as applied to claim 15 above, and further in view of Intel.

Regarding claim 37, Devine does not expressly teach enabling a legacy option ROM or translating the results of the I/O services into a native API.

Intel expressly teaches enabling a legacy option ROM to run and effect its input/output services ["*The PC industry has a huge investment in Intel Architecture Option ROM technology, and the obsolescence of this installed base of technology is not practical in the first generation of EFI-compliant system. The interfaces have been designed in such as way* [sic] *as to map back into legacy interfaces. These interfaces have in no way been burdened with any restrictions inherent to legacy Option ROMs.*" (page 14)].

Regarding the limitation of "translating the results of the I/O services into a native API," the disclosure of the instant application teaches (paragraph 0014):

> The VMM then translates the results [of the legacy option ROM running and effecting its I/O services] into a native API. That is, the VMM traps the I/O to the semantic equivalent in the native environment.

In a VMM which supports emulation of a non-native architecture, this is regarded as an inherent feature. Failure to perform this function would render the legacy option ROM inoperable in combination with the VMM. Therefore this limitation is an obvious detail of implementation of when combining support for a legacy option ROM with the invention of Devine.

It would have been obvious to combine support for a legacy option ROM with the invention of Devine for the reasons cited by Intel, specifically to enable support for legacy drivers which use legacy option ROMs when providing support for non-native operating system on a particular architecture. The combination would require adequate support in the VMM for the legacy devices which employ the legacy option ROMs, specifically "trapping the I/O to the semantic equivalent in the native environment". Failure to do so would produce an inoperable combination.

Allowable Subject Matter

Claims 27-29 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph and 35 U.S.C. § 101, set forth in this Office action. The allowable status of these claims, however, depends on the manner of clarification provided the use of a VMM for authenticating a firmware module.

Claims 30-32 and 35 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action, and rewritten in independent form including all of the limitations of the base claim and any intervening claims. The allowable status of these claims, however, depends on the manner in which the rejections under 35 U.S.C. § 112 are resolved.

Claims 36 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

12. The following is a statement of reasons for the indication of allowable subject matter: A search of the prior art fails to reveal or render obvious at least the combinations recited in claims 27, 30, 35, and 36. Specifically, the allowable subject matter resides in the combination of:

1) executing a VMM during the pre-boot phase of a computer system,

2) the computer system using an Extensible Firmware Interface, and

3) the VMM authenticating the Extensible Firmware Interface firmware modules.

The third element, authenticating the Extensible Firmware Interface (EFI) firmware modules, clearly implies the VMM performs a role of system security. While the prior art renders obvious executing a VMM during the pre-boot phase of a computer system in combination with an Extensible Firmware Interface, the prior art goes no further and fails to contemplate a VMM that provides system security by authenticating the EFI firmware modules.

A search of the prior art fails to expressly provide motivation to combine a pre-boot VMM in a computer system using an EFI and authenticating the EFI firmware modules with the

VMM. Motivation does not always have to come from within the prior art references. However, in the instant case, taking into consideration the nature of this art and the skill level required, one would need some impetus and direction to modify the individual teachings to result in the integrated steps as recited in the claims.

The prior art shown on the forms P.T.O. 892 and made of record, is the closest art uncovered during the examination process and is considered pertinent to Applicant's invention. Though considered pertinent, the art is not anticipatory and does not render obvious the claimed system as recited in claims 27, 30, 35, and 36.

Of the prior art made of record, the teachings considered by the examiner to be closest to Applicant's invention are found in Devine and Intel, cited under 35 U.S.C. §§ 102 and 103 in this Office Action. Devine teaches the use of a pre-boot VMM to execute non-native operating systems, non-native applications, and to implement a sandbox feature, while Intel teaches the use of an Extensible Firmware Interface and its contribution to executing operating systems on non-native platforms. Neither reference contemplates authenticating the EFI firmware modules with the pre-boot VMM.

Conclusion

Art considered pertinent by the examiner but not applied has been cited on form PTO-892.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason Proctor whose telephone number is (571) 272-3713. The examiner can normally be reached on 8:30 am-4:30 pm M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Leo Picard can be reached at (571) 272-3749. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-3713.

Any inquiry of a general nature or relating to the status of this application should be directed to the TC 2100 Group receptionist: 571-272-2100. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Proctor
Examiner
Art Unit 2123

jsp

W Thomson
Primary Examiner
TC 2100
AU 2123